Exchange Platinum in Exchange 5.5 Mixed Environments and Down Level NT4 Domains

Exchange Platinum in Exchange 5.5 Mixed Environments and Down Level NT4 Domains....1
Introduction....1
Ex2000 Connectivity Components....1
Active Directory Connector....1
Windows 2000 ADC vs Exchange 2000 ADC....2
Site Replication Service....2
RPC Connector....2
Interoperability Scenarios....2
Ex2000 in Separate Org from Ex5.5....3
Ex2000 in Same Ex5.5 Organization....3
Ex2000 Separate from Ex5.5 Sites....4
Ex2000 in Same Ex5.5 Sites....4
Ex2000 In Multiple Ex5.5 Sites....5
Issues You May Encounter....5
How to manage Exchange 5.5 and Exchange 2000 servers when in mixed mode....5
RPC Connectivity in Complex Domain Infrastructures....5
Exchange 5.5 Security Issues Using Windows 2000 Groups....6
Exchange 2000 and Win2000 Mixed/Native....6
Conclusion....7

Introduction

Ex2000 Connectivity Components

A noted is other chapters, there are several connectivity components that are added to the Exchange 2000 environment that allow it to communicated properly with an Exchange 5.5 organization. These include the Active Directory Connector, which allows replication of directory information between the Windows 2000 Active Directory and the Exchange 5.5 directory; the Exchange 2000 Site Replication Service, which allows the Exchange 2000 system to look like an Exchange 5.5 system to the rest of the Exchange 5.5 organization; and the Exchange 2000 RPC Connector, which allows the Exchange 2000 server to communicate with ***

Active Directory Connector

The Active Directory Connector is used to replicate directory information between the Exchange 5.5 directory and the Windows 2000 Active Directory. When you connect your Exchange 5.5

organization to your Windows 2000 AD, you will create at least one ADC Connection Agreement to pass the user information between the two directories. Note that there are basically two implementations of the ADC, one for connecting just Windows 2000 to the Exchange 5.5 directory, and one for connecting Exchange 5.5 and Exchange 2000. The former of these is a subset of the latter, so if you don't install the Windows 2000 ADC, it will be installed when you install the Exchange 2000 ADC.

Windows 2000 ADC vs Exchange 2000 ADC

As stated above, the Windows 2000 ADC is a subset of the Exchange 2000 ADC. It allows only directory replication of mailboxes, custom recipients, and distribution lists from Exchange 5.5 to the Windows 2000 AD and of accounts, contacts, and groups from the Windows 2000 AD to the Exchange 5.5 directory.

The Exchange 2000 ADC adds the ability to exchange configuration information of the Exchange 5.5 organization with the Windows 2000 AD, and of Exchange 2000 configuration information (from the Windows 2000 AD) to the Exchange 5.5 organization. Regardless of the CAs created for the Windows 2000 ADC, this ADC creates a read-only Configuration CA that performs this bi-directional configuration information transfer.

Site Replication Service

The Exchange 2000 SRS allows the Exchange 2000 server to more closely resemble an Exchange 5.5 server. It includes the same dir.edb that is used on all Exchange 5.5 servers for directory services, and is in fact used as the Exchange 2000 side of the ADC ConfigCA.

While in mixed-mode, all Connection Agreements must specify the Exchange 2000 server that is running SRS. This is specified under the Active Directory Connector Management > Connection Agreement > Connection tab > Server.

For further information about the SRS, please refer to chapter XXX, <chapter title>, of this guide.

RPC Connector

The RPC connector is used to connect the Exchange 2000 systems to the Exchange 5.5 systems for message transfer. Note that this

connector is only used within the mixed Exchange site, not for message transfer between Exchange sites, whether they are mixed or pure.

Interoperability Scenarios

Obviously, if you are currently running Exchange 5.5, there is only one way you aren't going to run into one of the following interoperability scenarios, and that is if you have a single server and upgrade it directly to Windows 2000 and Exchange 2000. Other than that scenario, we have tried to come up with the configurations we feel will be encountered most often in the current Exchange organizations.

Ex2000 in Separate Org from Ex5.5

Since "by default" Exchange 5.5 is in a different "organization" from the Exchange 2000 organization, the "separate organization" spoken of in this section refers to an Exchange 5.5 organization that is not part of the Exchange 5.5 organization that was originally connected to the Exchange 2000 organization. With this in mind, connecting these two organizations is little different from connecting two Exchange organizations at any version.

For directory interoperability between these organizations, we recommend that the Windows 2000 ADC be used in Interorganizational Mode, which is set on the <Advanced??> property page of the ADC CAs that are created. This allows the directories of the two organizations to be shared, allowing full GAL lookup and access on either side of the ADC CA.

For mail transfer between the organizations, the most likely avenue is to create an SMTP connector between the two organizations and use it for all mail transfer. Though the X.400 connector can also be used, and either connector can handle the type of traffic this connector will need to support, the SMTP connector is native to Exchange 2000, and is typically easier to configure in both environments. ~~Note, however, that since the final configuration is going to be to move toward Exchange 2000, and since the SMTP connector can be configured easier, the more logical connection to use would be the SMTP connection.~~ Below is a simple diagram of this sort of organization, before and after implementing the connectors required for interoperability.

Ex2000 in Same Ex5.5 Organization

In the next sections, we are going to explore how Exchange 5.5 and Exchange 2000 can coexist in the same organizational structure. Note that when an Exchange 2000 server is built into an Exchange 5.5 organization, several Exchange 2000 capabilities are not available. For instance, as long as there is an Exchange 5.5 server in the organization, all Exchange 2000 Routing Groups are directly tied to a specific Exchange 2000 Administrative Group, and all Exchange Administrative Groups can only host a single Routing Group. This one-for-one relationship is required so that the Exchange 5.5 servers can "understand" the configuration. They use this strict configuration to map Exchange 2000 RG/AG combinations to Exchange 5.5 Sites, which are displayed as such in the Exchange 5.5 administrative tools.

For those organizations that are upgrading their Exchange 5.5 organizations, there are several possible configurations that they might wish to consider. The first, one where the Exchange 2000 servers are in purely Exchange 2000 RG/AG from the Exchange 5.5 sites, closely resembles that of the previous section. The major difference between these is in how the Exchange 2000 organization is built. The Exchange 2000 organization maps the Exchange 5.5 Sites to Exchange 2000 RG/AGs. This can be done by having Exchange 2000 servers segregated from Exchange 5.5 servers (effectively creating Exchange 2000 "Sites"), or by joining the Exchange 2000 servers into the Exchange 5.5 sites. The following sections deal with these different scenarios.

Ex2000 Separate from Ex5.5 Sites

Since it resembles the Exchange 5.5 in separate organization configuration, all of the directory and messaging transfer configuration details apply with the following exception: You will install the ADC in the single organization mode.

As with the previous configuration, either the SMTP or X.400 connection can be used in this configuration. And again, the most logical connection is the SMTP connection.

Ex2000 in Same Ex5.5 Sites

Unlike the previous examples, an Exchange 2000 server in the current Exchange 5.5 sites uses a direct RPC connection for messaging traffic between the different server versions. Additionally, since the Exchange 2000 server(s) will have to participate in the Exchange 5.5

directory replication, one of these will have to host the Site Replication Service (SRS). This will allow direct directory transfer between the two systems, and both will be logically in the same actual organization (not just a logical connection, as was the case previously). The following sections deal with these differences in more details.

Ex2000 Messaging in an Ex5.5 Site

Since the primary means of message transfer between servers in an Exchange 5.5 site is direct RPC transfer, and all servers will send directly to each server in the same site, all Exchange 2000 servers in a mixed-mode site must be able to send and receive messages directly from these Exchange 5.5 servers.

This is accomplished by …

Ex2000 Directory in an Ex5.5 Site

In addition to using the standard ADC Connection Agreements for replication of mailbox, distribution list, and custom recipient information (to Windows 2000 accounts, groups and contacts), Exchange 2000 adds two other directory tools. The first is a Configuration Connection Agreement (C-CA), which passes the actual Exchange 5.5 organization information into the Windows 2000 Active Directory (and the Exchange 2000 server information back). This allows the Exchange directory to reflect that there are Exchange 2000 servers in the Exchange 5.5 site, and allows some access to these servers.

The second, the SRS, allows an Exchange 2000 server to actually look like an Exchange 5.5 server from the Exchange 5.5 organization. This service builds a copy of the Exchange 5.5 directory, the dir.edb, right on the Exchange 2000 server, which is updated from and updates the Exchange 5.5 servers the same way they update each other – direct RPC communication. It also extends the access built by the C-CA by allowing direct RPC access to the Exchange 2000 servers from the Exchange 5.5 Admin console. Not all objects are accessible (you can see the different mailbox databases on the server, but you can't see the actual mailboxes at the server level), but it makes access to the Exchange 2000 servers more admin-friendly.

Ex2000 In Multiple Ex5.5 Sites

This is the most elaborate mixed-Exchange configuration. However, it is just an extension of the previous. There are multiple sites, so there are multiple C-CAs (one for each site), and there are multiple SRS servers, again at least one for each site.

Note that there is a possibility for the Exchange 5.5 servers to be removed from these sites, leaving what might seem like two Exchange 5.5 sites with no Exchange 5.5 servers. However, since the Exchange 2000 servers not only replicate via the Exchange 5.5 directory, but also use the Windows 2000 Active Directory for this information transfer, they will know when they are "talking" directly to other Exchange 2000 servers, and will use the Active Directory rather than the Exchange 5.5 directory. **(This is still being fleshed out, so we don't have details of how it will work. Please stay tuned.)**

Issues You May Encounter

How to manage Exchange 5.5 and Exchange 2000 servers when in mixed mode

It is recommended that all Exchange 5.5 servers are continued to be managed from the existing Exchange 5.5 administrator program and that all Exchange 2000 servers are managed from Exchange 2000's system manager.

There are several errors that may arise if you attempt to manage Exchange 5.5 from Exchange 2000's system manger or manage Exchange 2000 from Exchange 5.5's administrator program.

Windows NT/Exchange 2000 ADC Active Directory account duplication

When using the Exchange 2000 ADC you create Windows 2000 accounts based on your existing Exchange 5.5 mailboxes and NT 4 accounts. An issue may arise where there are duplicate accounts for one individual. This can come about from using additional migration tools such as upgrading an NT 4 domain to Windows 2000 prior to install the Exchange 2000 ADC.

There is a domain clean up tool available that will search for duplicate accounts and merge these accounts if need be based on an administrators selection.

RPC Connectivity in Complex Domain Infrastructures

In a complex infrastructure, Exchange requires that certain accounts and all Exchange servers have permissions in not only the Active Directory domains and schema, but in at all levels of the Exchange 5.5 organization. The Exchange 2000 Setup application sets all the proper permissions in the Windows 2000 Active Directory *(note: at least it will by RTM, and may in newer builds than Beta 3)*. If you are seeing problems with mail communications between Exchange 5.5

servers and Exchange 2000 servers, check the permissions and see that the Exchange 2000 Servers group has been granted Service Account Admin permission to all levels of the Exchange 5.5 organization.

Exchange 5.5 Security Issues Using Windows 2000 Groups

If your Exchange 5.5 servers are on Windows NT 4.0, you will not be able to use nested global groups in your Exchange architecture. Since Exchange gets its reference to this security information from the underlying Windows NT infrastructure, and since the NT 4.0 servers can't understand nested global groups, any users in these groups may not receive the permissions you expect them to have on your Exchange 5.5 organization. For instance, if you have two groups, Enterprise Admins and Domain Admins, and you decide to put the Domain Admins into the Enterprise Admins group, then use the Enterprise Admins to grant security to the Exchange 5.5 organization, any users in either the Domain Admins or the Enterprise Admins group might not have the permissions you expect them to have.

Another aspect where you expect certain securities to be granted is if you are using Exchange 5.5 DLs to grant permissions to Exchange 5.5 objects. For instance, if you have granted permissions to an Exchange 5.5 Public Folder to an Exchange 5.5 DL, since DLs have no security at the Windows NT level, these Exchange 5.5 DLs will have to be translated to Windows 2000 security groups, and in most cases universal groups, to allow them to have the same permissions they had in the Exchange 5.5 public folder structure. Note that you may wish to nest global groups in individual domains into the universal groups that are used to grant/deny permissions in this fashion. This will allow you to limit how much data is replicated to the Global Catalogue servers if your DL was large in the Exchange 5.5 system. Also note that using this approach will not work if you have Windows NT 4.0 servers in your overall Exchange organization, regardless of the NT domain they reside in. (See the previous note on nested groups.)

Exchange 2000 and Win2000 Mixed/Native

There are several modes and combination of modes that you can be in with both Windows 2000 and Exchange 2000. There is a Windows 2000 mixed-mode and native-mode and there is also an Exchange 2000 mixed-mode and native-mode. Exchange 2000's mode is not related to which mode Windows 2000 is in but there are some

implications of being in Windows 2000 mixed-mode while running Exchange 2000.

Windows 2000 mixed-mode
Being in Windows 2000 mixed-mode means you still have some downlevel NT 4 BDCs in your Windows 2000 domain. The primary reason for this mode is so you can provide backward compatibility with NT 4 domain controllers. Once all of your NT 4 domain controllers are upgraded to Windows 2000 you can manually make the switch to Windows 2000 native mode. Two cautions about the previous statement: This is a one-way operation and is not reversible, and if you are running Exchange 5.5 on clustered servers in the upgraded domain, you must maintain the mixed-mode environment.

Windows 2000 Mixed-mode implications on Exchange 2000
When Windows 2000 is in mixed-mode, your email-enabled security groups are limited to global groups and computer local groups. You can create non-security based groups, called distribution groups, for things such as distribution lists but this may lead to having two of the same group, one for email and one for security. You should carefully plan your when you create mail enabled distribution groups (non-security related) vs. mail enabled security enabled groups to avoid duplication. If you email-enable both type of groups, both will show up in an Exchange 2000 address list. The ability to utilize one group for email and security permissions is a very attractive concept with Exchange 2000 since you don't have to manage two sets of groups.

Another limitation of being in Windows 2000 mixed-mode is you cannot nest email enabled security groups in mixed mode. Nesting of security groups is only available in Windows 2000 native mode. It is also a good rule of thumb to limit your mailboxes listed in mail-enabled security groups to 5,000. If you have a need for a company wide mail-enabled security group or distribution list that will be more than 5,000 mailboxes, for example, then it is recommended you use nested groups within this company wide group.

Windows 2000 native-mode
Once you switch your Windows 2000 domain to full native mode, you can now create additional types of email enabled groups for Exchange 2000. These additional groups include: domain local groups and universal groups.

Exchange 2000 Mixed-mode
When Exchange 2000 is first installed, the default mode is mixed-mode even if you don't have previous versions of Exchange in your

Exchange organization. The primary reason for this mode is if you still have servers earlier versions of Exchange within your Exchange 2000 organization. You cannot switch to full native Exchange 2000 mode until each previous version of Exchange server is upgraded to Exchange 2000.

While in mixed-mode, each of your Exchange 5.5 sites map directly to an Exchange administrative group and routing group respectively. You cannot easily move servers amongst groups while in this mode nor can you easily move user mailboxes between administration groups. Additionally, the Exchange 2000 routing group objects are not available and you cannot rename administrative groups *(note to editor: the renaming may be beta limitation)*

Conclusion

Though there is not going to be a standard environment for a mixed Exchange 5.5/ Exchange 2000 system, we have tried to show how several of the most common configurations our customers currently have deployed could coexist and later be migrated to Windows 2000 and Exchange 2000. In none of these cases do we feel that the connections between the two messaging systems is trivial – to the contrary, even the simplest multi-server Exchange 5.5 environment will take a lot of planning before it can be joined to, and finally migrated to, Exchange 2000.